UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

NILS MÖLDER, Individually and On Behalf of All Others Similarly Situated,

Plaintiff,

v.

UBIQUITI INC., ROBERT J. PERA, and KEVIN RADIGAN,

Defendants.

Case No. 1:21-cv-04520-DLC

SECOND AMENDED CLASS ACTION COMPLAINT FOR VIOLATIONS OF THE FEDERAL SECURITIES LAWS

JURY TRIAL DEMANDED

Lead Plaintiff Irit Lukomski ("Plaintiff"), individually and on behalf of all others similarly situated, by and through her attorneys, alleges the following upon information and belief, except as to those allegations concerning Plaintiff, which are alleged upon personal knowledge. Plaintiff's information and belief is based upon, among other things, her counsel's investigation, which includes without limitation: (a) review and analysis of regulatory filings made by Ubiquiti Inc. ("Ubiquiti" or the "Company") with the United States ("U.S.") Securities and Exchange Commission ("SEC"); (b) review and analysis of press releases and media reports issued by and disseminated by Ubiquiti; and (c) review of other publicly available information concerning Ubiquiti.

I. NATURE OF THE ACTION AND OVERVIEW

1. This is a class action on behalf of persons and entities that purchased Ubiquiti securities on the NYSE (the "Class")[1] between January 11, 2021 and March 30, 2021, inclusive (the "Class Period"). Plaintiff pursues claims under the Securities Exchange Act of 1934 (the "Exchange Act").

2. Ubiquiti develops and markets equipment and technology platforms for high-capacity internet access, unified information technology, and consumer electronics. In addition to being one of the biggest sellers of networking gear, the Company designs and sells many cloud-enabled devices such as wifi routers, video surveillance systems, and electronic door locks that customers can access remotely over the internet.

[1] Excluded from the Class are: Defendants and their immediate families; the officers and directors of Ubiquity at all relevant times; their subsidiaries, affiliates, legal representatives, heirs, successors, or assigns; and any entity in which Defendants or any excluded persons have or had a controlling interest.

3. On January 11, 2021, Ubiquiti announced that they had detected a data breach in a short email to customers:

> Dear Customer,
>
> We recently became aware of unauthorized access to certain of our information technology systems hosted by a third party cloud provider. We have no indication that there has been unauthorized activity with respect to any user's account.
>
> We are not currently aware of evidence of access to any databases that host user data, but we cannot be certain that user data has not been exposed. This data may include your name, email address, and the one-way encrypted password to your account (in technical terms, the passwords are hashed and salted). The data may also include your address and phone number if you have provided that to us.
>
> As a precaution, we encourage you to change your password. We recommend that you also change your password on any website where you use the same user ID or password. Finally, we recommend that you enable two-factor authentication on your Ubiquiti accounts if you have not already done so.
>
> We apologize for, and deeply regret, any inconvenience this may cause you. We take the security of your information very seriously and appreciate your continued trust.
>
> Thank you,
> Ubiquiti Team

4. That same day, major tech publications, including *Tech Crunch*,[2] *The Verge*,[3] and *ZDNet*,[4] as well as popular internet forums such as Reddit.com[5] republished the letter to customers on their websites. Ubiquiti also placed a copy of the letter on its own website.[6]

---

[2] https://techcrunch.com/2021/01/11/ubiquiti-says-customer-data-may-have-been-accessed-in-data-breach/ (last accessed on November 9, 2021).

[3] https://www.theverge.com/2021/1/11/22226061/ubiquiti-data-breach-email-third-party-unathorized-access (last accessed on November 9, 2021).

[4] https://www.zdnet.com/article/ubiquiti-tells-customers-to-change-passwords-after-security-breach/ (last accessed November 9, 2021).

[5] *E.g.*, https://www.reddit.com/r/Ubiquiti/comments/kv9fc8/ubiquiti_email_re_breach/ (last accessed November 9, 2021).

[6] https://community.ui.com/questions/Account-Notification/96467115-49b5-4dd6-9517-f8cdbf6906f3 (last accessed on November 9, 2021).

5. On March 30, 2021, at around 2 pm ET, the well-regarded IT Security reporter Brian Krebs ("Krebs") posted an article on his website, Krebs on Security, entitled "Whistleblower: Ubiquiti Breach 'Catastrophic'", and revealing that the January 11 data breach was far more severe than Ubiquiti had previously disclosed.[7] The article explained that the "third-party cloud provider claim was a fabrication." According to a security professional at Ubiquiti who had helped the Company respond to the breach beginning in December 2020, whom Krebs called "Adam," the attackers had accessed "privileged credentials that were previously stored in the LastPass account of a Ubiquiti IT employee, and gained root administrator access to all Ubiquiti AWS [Amazon Web Services] accounts, including all S3 data buckets, all application logs, all databases, all user database credentials, and secrets required to forge single sign-on (SSO) cookies."

6. Adam reached out to Krebs after raising his concerns with Ubiquiti's whistleblower hotline and with the European data protection authorities. In his letter to the European Data Protection Supervisor, Adam stated that "[the breach] was catastrophically worse than reported, and legal silenced and overruled efforts to decisively protect customers[.] … The breach was massive, customer data was at risk, access to customers' devices deployed in corporations and homes around the world was at risk."

7. On this news, the Company's stock price fell $27.78 per share, or 7.4%, on March 30, 2021, continued to fall another $50.70 per share, or 14.5%, on March 31, 2021, to close at $298.30 on March 31, 2021, and fell another $9.15 per share, or 3%, to close at $289.15 per share on April 1, 2021, all on unusually heavy trading volume.

---

[7] https://krebsonsecurity.com/2021/03/whistleblower-ubiquiti-breach-catastrophic/ (last accessed on November 9, 2021).

8. Throughout the Class Period, Defendants made false and/or misleading statements of material fact, as well as failed to disclose material adverse facts about the Company's business, operations, and prospects that made their statements misleading. Specifically, Defendants, in their statements concerning the data breach, failed to speak fully and truthfully because: (1) the Company misleadingly downplayed the severity of the data breach in January 2021; (2) the Company failed to disclose that attackers had obtained administrative access to Ubiquiti's servers and obtained access to, among other things, all databases, all user database credentials, and secrets required to forge single sign-on (SSO) cookies; (3) as a result, intruders already had credentials needed to remotely access Ubiquiti's customers' systems; and (4) as a result, Defendants' misled investors as to the true risks to the Company's network infrastructure, customer data, privacy and safety, and the reputational and financial harm Ubiquiti would suffer.

9. As a result of Defendants' wrongful acts and omissions, and the precipitous decline in the market value of the Company's securities, Plaintiff and other Class members have suffered significant losses and damages.

II. JURISDICTION AND VENUE

10. The claims asserted herein arise under and pursuant to Sections 10(b) and 20(a) of the Exchange Act (15 U.S.C. §§ 78j(b) and 78t(a)) and Rule 10b-5 promulgated thereunder by the SEC (17 C.F.R. § 240.10b-5).

11. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 and Section 27 of the Exchange Act (15 U.S.C. § 78aa).

12. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391(b) and Section 27 of the Exchange Act (15 U.S.C. § 78aa(c)). Substantial acts in furtherance of the alleged fraud or the effects of the fraud have occurred in this Judicial District. Many of the acts charged herein, including the dissemination of materially false and/or misleading information, occurred in

substantial part in this Judicial District. In addition, the Company's principal executive offices are in this Judicial District and Ubiquiti's common stock trades on the New York Stock Exchange ("NYSE"), located within this Judicial District.

13. In connection with the acts, transactions, and conduct alleged herein, Defendants directly and indirectly used the means and instrumentalities of interstate commerce, including the United States mail, interstate telephone communications, and the facilities of a national securities exchange.

III. PARTIES

14. Plaintiff Irit Lukomski, as set forth in the certification previously filed with the Court, incorporated by reference herein (Dkt. No. 11-2), purchased Ubiquiti securities during the Class Period, and suffered damages as a result of Defendants' violations of the federal securities laws.

15. Defendant Ubiquiti is incorporated under the laws of Delaware with its principal executive offices located at 685 Third Avenue, 27th Floor, New York, New York 10017. Ubiquiti's common stock trades in an efficient market on the NYSE under the symbol "UI."

16. Defendant Robert J. Pera ("Pera") has served as the Chief Executive Officer ("CEO") and a member of the Board of Directors since Ubiquiti's inception, and as the Chairman of the Board since December 2012. Pera founded Ubiquiti in October 2003.

17. Defendant Kevin Radigan ("Radigan") has served as the Chief Accounting and Finance Officer since May 2016. Before joining Ubiquiti, Radigan was the Chief Financial Officer at American Medical Alert Corp. from January 2012 to March 2016, and previously served in various financing and accounting positions both in the electronics and pharmaceuticals industries.

18. Defendants Pera and Radigan are sometimes referred to collectively herein as the "Individual Defendants".

19. The Individual Defendants, because of their high-ranking positions, their job responsibilities, and direct involvement in the everyday business of the Company, possessed the power and authority to control the contents of the Company's reports to the SEC, press releases and other public statements, and presentations to securities analysts, money and portfolio managers and institutional investors, *i.e.*, the market.

20. The Individual Defendants were provided with copies of the Company's reports and press releases alleged herein to be misleading prior to, or shortly after, their issuance and had the ability and opportunity to prevent their issuance or cause them to be corrected. Because of their positions and access to material non-public information available to them, the Individual Defendants knew that the adverse facts specified herein had not been disclosed to, and were being concealed from, the public, and that the positive representations which were being made were then materially false and/or misleading.

21. The Individual Defendants are liable for the false statements and omissions pleaded herein, as those statements were each "group-published" information, the result of the collective actions of the Individual Defendants.

IV. DESCRIPTION OF THE FRAUD

A. Background Of The Company And Its Business

22. Ubiquiti develops and markets equipment and technology platforms for high-capacity internet access, unified information technology, and consumer electronics. Ubiquiti targets three types of clients: internet service providers, enterprises, and consumers. Among its products are wifi routers, internet connected video surveillance systems, internet connected door locks, and devices to ensure network security.

23. In its annual report on Form 10-K for the 2020 fiscal year, Ubiquiti stated that it markets its products through a "highly engaged community of service providers, distributors, value

added resellers, systems integrators and corporate IT professionals, which we refer to as the Ubiquiti Community." Ubiquiti does not employ a traditional sales force, but "instead drive[s] brand awareness through online reviews and publications, [Ubiquiti's] website, [its] distributors and the Company's user community where customers can interface directly with our R&D, marketing, and support teams. [Ubiquiti's] technology platforms were designed from the ground up with a focus on delivering highly-advanced and easily deployable solutions that appeal to a global customer base market."

24. Pera, as Ubiquiti's CEO, Chairman, founder, and majority owner, actively runs the Company. He stated at a September 26, 2017 Investor Day presentation that "I don't want to be the leader in the movies that sits up high in a castle and watches all of his soldiers, who he feels expendable get killed off one by one. I want to be the guy leading by example. I want to be the guy on the battlefield. And I think that top-down accountability is very important because when you have the small teams and something goes wrong, the worst thing for culture is somebody saying, 'Well, that's not my job.' If somebody sees a problem, they have to attack it. Just like I attack it. I don't consider myself lower -- above any job. I'll go into the forums, I'll go into the lab, I'll rework products, I don't care. I want that culture. And that's why I do the things I do."

25. Ubiquiti states that as its founder, Chairman, CEO, and majority owner, Pera "is able to exercise voting rights with respect to a majority of the voting power of our outstanding stock and therefore has the ability to control the outcome of matters submitted to our stockholders for approval, including the election of directors. . . . In addition, Mr. Pera has the ability to control the management and major strategic investments of our company as a result of his position as our [CEO] and his ability to control the election or replacement of our directors. . . . As a board member and officer, Mr. Pera owes a fiduciary duty to our stockholders and must act in good faith in a

manner he reasonably believes to be in [their] best interests. . . . As a stockholder, even a controlling stockholder, Mr. Pera is entitled to vote his shares in his own interests, which may not always be in the interests of our stockholders generally."

B. Ubiquiti's Use Of Amazon Web Services For Cloud Based Devices

26. Rather than rely on their own servers for their data and processing needs, Ubiquiti relies on third party service providers, including Amazon Web Services "to provide distributed computing infrastructure platforms for business operations, or what is commonly referred to as a 'cloud' computing service." Ubiquiti uses Amazon Web Services, among other purposes, to give customers remote access over the internet to control Ubiquiti's products. So, for instance, a customer who uses these cloud services could monitor their video surveillance feed, check the internet usage of their home wifi network, or even lock and unlock their doors from anywhere they can connect to the internet.

27. For the convenience of its customers, Ubiquiti created a "single sign-on" ("SSO") system, whereby a user can create a single account to access multiple Ubiquiti devices they own.

28. Also for the convenience of its customers, Ubiquiti also uses a technology called a single sign-on cookie. In the context of internet technology, a "cookie" is a piece of code that a web based service such as a website leaves on a user's computer or device to allow the web service to identify that user's computer or device in the future. The single sign-on cookie that Ubiquiti uses allows Ubiquiti's various web services to recognize a particular computer or device as belonging to a user after that user signs in once. That allows the user to not have to sign into Ubiquiti every time they access a Ubiquiti service.

C. Ubiquiti's Networks Are Breached, And Ubiquiti Concealed The Extent Of The Hack

29. On January 11, 2021, Ubiquiti sent an email to customers and also published it on their website stating that it had become aware of "unauthorized access to certain of our information technology systems hosted by a third party cloud provider." It stated:

> Dear Customer,
>
> We recently became aware of unauthorized access to certain of our information technology systems hosted by a third party cloud provider. We have no indication that there has been unauthorized activity with respect to any user's account.
>
> ***We are not currently aware of evidence of access to any databases that host user data, but we cannot be certain that user data has not been exposed.*** This data may include your name, email address, and the one-way encrypted password to your account (in technical terms, the passwords are hashed and salted). The data may include your address and phone number if you have provided that to us.
>
> As a precaution we encourage you to change your password. We recommend that you also change your password on any website where you use the same user ID or password. Finally, we recommend that you enable two-factor authentication on your Ubiquiti accounts if you have not already done so.
>
> We apologize for, and deeply regret, any inconvenience this may cause you. We take the security of your information very seriously and appreciate your continued trust.
>
> Thank you,
>
> Ubiquiti Team

30. Major tech websites including *Tech Crunch*, *The Verge*, and *ZDNet* republished the letter to customers on their websites that same day, as well as popular internet forums such as Reddit.com, where Ubiquiti users discussed the potential data breach and their disappointment in the lack of transparency Ubiquiti provided in the email.

31. However, the truth is that the hack against Ubiquiti was much more severe than Ubiquiti admitted. The truth came to light due to the reporting of cybersecurity expert and former

Washington Post journalist Brian Krebs ("Krebs"), who authors the blog "Krebs on Security".[8] Krebs reported that "[a] security professional at Ubiquiti who helped the company respond to the two-month breach beginning in December 2020 contacted KrebsOnSecurity after raising his concerns with both Ubiquiti's whistleblower hotline and with European data protection authorities." Because Krebs' source feared retribution, Krebs referred to him only as "Adam". According to Adam, the breach "was catastrophically worse than reported, and legal silenced and overruled efforts to decisively protect customers … The breach was massive, customer data was at risk, access to customers' devices deployed in corporations and homes around the world was at risk."

---

[8] Krebs on Security, a computer security and cybercrime blog, is published by Brian Krebs, an American journalist and investigative reporter, best known for his coverage of profit-seeking cybercriminals. Krebs worked as a reporter for The Washington Post from 1995 to 2009, where he authored more than 1,300 blog posts for the Security Fix blog, as well as hundreds of stories for washingtonpost.com and The Washington Post newspaper, including eight front-page stories in the paper edition and a Post Magazine cover piece on botnet operators. Among others, Krebs first broke the news on Target's major data breach announced by Target on December 19, 2013, one day after Krebs reported on his "Krebs on Security" blog that Target was investigating this data breach and citing "reliable sources." *See* https://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/ (last accessed November 9, 2021). A January 16, 2014 Bloomberg article describes Krebs as follows:

> Krebs's talent for exposing the weaknesses in online security has earned him respect in the IT business and loathing among cybercriminals. His track record of scoops, including the Dec. 18 revelation that hackers stole tens of millions of customers' financial data from Target, has helped him become the rare blogger who supports himself on the strength of his reputation for hard-nosed reporting. … Krebs often posts step-by-step details—without outing his sources—of how he's uncovered which hackers breached whose corporate defenses. "That's something people really want," says Andy Ellis, chief security officer at Akamai Technologies. "Everything he writes is some of our best open-source intelligence."

Karen Weise, *Brian Krebs, the Cybersecurity Blogger Hackers Love to Hate*, BLOOMBERG, Jan. 16, 2014, available at https://www.bloomberg.com/news/articles/2014-01-16/brian-krebs-the-cybersecurity-blogger-hackers-love-to-hate.

32. Krebs went on to report that "[a]ccording to Adam, the hackers obtained full read/write access to Ubiquiti databases at Amazon Web Services (AWS), which was the alleged 'third party' involved in the breach."

33. Krebs further reported that, according to Adam, they were able to obtain full administrative access, which allowed them to obtain "cryptographic secrets for single sign-on cookies and remote access, full source code control contents, and signing keys exfiltration,"

34. Krebs explained that "[s]uch access could have allowed the intruders to remotely authenticate to countless Ubiquiti cloud-based devices around the world. According to its website, Ubiquiti has shipped more than 85 million devices that play a key role in networking infrastructure in over 200 countries and territories worldwide." That is, the hackers had the ability to pose as the owner of any Ubiquiti device anywhere and gain full access to it. However, Ubiquiti was unable to determine exactly what user accounts were accessed because "Ubiquiti had negligent logging (no access logging on databases) so it was unable to prove or disprove what [the hacker] accessed." Ubiquiti's failure to maintain access logging on databases was both contrary to the standard operating procedures of large tech companies and contrary to the interests of its customers. Access logs are a basic piece of a server operator's infrastructure because they allow the company to track who accessed their servers, when, and what they accessed. Among other things, maintaining such logs allows the server operator to determine what could have caused errors or problems with the server. In addition, access logging would allow a company that is the victim of a cyberattack to determine just what the attacker accessed and therefore what exposure customers face. Therefore, failure to maintain such logs is negligent.

35. According to Adam, the legal department interfered with efforts to better protect Ubiquiti customers and to honestly inform the public of what was happening. "Legal overrode the

repeated requests to force rotation of all customer credentials, and to revert any device access permission changes within the relevant period." That is, the legal department stopped Ubiquiti security employees from automatically resetting all customers' login information so as to keep out any hackers. Adam further explained that "Ubiquiti's breach disclosure … was 'downplayed and purposefully written to imply that a 3rd party cloud vendor was at risk and that Ubiquiti was merely a casualty of that, instead of the target of the attack.'"

36. The next day, on March 31, 2021, after the close of trading, Ubiquiti issued a statement on their website[9] that denied *none* of the allegations in Krebs on Security's reporting, but instead explained the tortuous logic by which they justified their earlier statement that they were unaware of evidence that customer data was accessed in the data breach, essentially admitting to everything Krebs on Security reported:

> As we informed you on January 11, we were the victim of a cybersecurity incident that involved unauthorized access to our IT systems. Given the reporting by Brian Krebs, there is newfound interest and attention in this matter, and we would like to provide our community with more information.
>
> At the outset, please note that nothing has changed with respect to our analysis of customer data and the security of our products since our notification on January 11. In response to this incident, we leveraged external incident response experts to conduct a thorough investigation to ensure the attacker was locked out of our systems.
>
> These experts identified no evidence that customer information was accessed, or even targeted. The attacker, who unsuccessfully attempted to extort the company by threatening to release stolen source code and specific IT credentials, never claimed to have accessed any customer information. This, along with other evidence, is why we believe that customer data was not the target of, or otherwise accessed in connection with, the incident.
>
> At this point, we have well-developed evidence that the perpetrator is an individual with intricate knowledge of our cloud infrastructure. As we are cooperating with law enforcement in an ongoing investigation, we cannot comment further.

[9] https://community.ui.com/questions/Update-to-January-2021-Account-Notification/3813e6f4-b023-4d62-9e10-1035dc51ad2e (last accessed on November 9, 2021).

> All this said, as a precaution, we still encourage you to change your password if you have not already done so, including on any website where you use the same user ID or password. We also encourage you to enable two-factor authentication on your Ubiquiti accounts if you have not already done so.
>
> Thanks,
>
> Team UI

37. But, as Krebs on Security noted in an update to the original article,[10] "Ubiquiti said its security experts identified 'no evidence that customer information was accessed, or even targeted.' Ubiquiti can say this, says Adam, because it failed to keep records of which accounts were accessing that data." Basic principles of data security dictate keeping logs of which accounts are accessing sensitive data such as customer information. This is to prevent this exact sort of situation from emerging – where a company cannot say whether sensitive data has been accessed because they did not keep any records. Essentially, Ubiquiti kept its head in the sand, leaving it unable to tell customers if their accounts had been accessed.

38. That same day, March 31, 2021, the tech news website *The Verge* published an article[11] criticizing Ubiquiti's response to the breach and to *Krebs on Security's* reporting:

> Ubiquiti, a company whose prosumer-grade routers have become synonymous with security and manageability, is being accused of covering up a "catastrophic" security breach — and after 24 hours of silence, the company has now issued a statement that doesn't deny any of the whistleblower's claims.
>
> Originally, Ubiquiti emailed its customers about a supposedly minor security breach at a "third party cloud provider" on January 11th, but noted cybersecurity news site KrebsOnSecurity is reporting that the breach was actually far worse than Ubiquiti let on. A whistleblower from the company who spoke to Krebs claimed that Ubiquiti itself was breached, and that the company's legal team prevented efforts to accurately report the dangers to customers.

---

[10] https://krebsonsecurity.com/2021/03/whistleblower-ubiquiti-breach-catastrophic/ last accessed on November 11, 2021).

[11] https://www.theverge.com/2021/3/31/22360409/ubiquiti-networking-data-breach-response-whistleblower-cybersecurity-incident (last accessed on November 9, 2021).

> It's worth reading Krebs' report to see the full allegations, but the summary is that hackers got full access to the company's AWS servers — since Ubiquiti allegedly left root administrator logins in an LastPass account — and they could have been able to access any Ubiquiti networking gear that customers had set up to control via the company's cloud service (now seemingly required on some of the company's new hardware).
>
> "They were able to get cryptographic secrets for single sign-on cookies and remote access, full source code control contents, and signing keys exfiltration," the source told Krebs.
>
> When Ubiquiti finally issued a statement this evening, it wasn't a reassuring one — it's wildly insufficient. The company reiterated its point that it had no evidence to indicate that any user data had been accessed or stolen. But as Krebs points out, the whistleblower explicitly stated that the company doesn't keep logs, which would act as that evidence, on who did or didn't access the hacked servers. Ubiquiti's statement also confirms that the hacker did try to extort it for money, but doesn't address the allegations of a cover up.
>
> …
>
> The other thing you'll notice is that Ubiquiti is no longer pinning this on a "third party cloud provider." The company admits that its own IT systems were accessed. But it doesn't address much else, and the fact that the statement confirms some of what the whistleblower said while leaving the most worrying parts (e.g., the alleged cover-up, lack of logs, poor security practices, etc.) unaddressed makes me uncomfortable to be a Ubiquiti owner.
>
> The company's networking gear is (or was) trusted by many techies, myself included, because it promised full control over your home or small business network, without the fears of cloud-based solutions.
>
> Throughout this process, Ubiquiti has failed to communicate properly with its customers. The fact that it's not denying the allegations, and indicates that they could be true, suggests that the original email was, at the very least, an insufficient warning. It encouraged users to change their passwords — according to Krebs, a more appropriate response would be immediately locking all accounts and requiring a password reset. Even today, the company is simply encouraging users to change their passwords and enable two-factor authentication.

39. On April 1, 2021, Credit Suisse published an analysis on the news titled "Not An April's Fools' Joke, January 2021 Security Breach May Be Worse Than Initially Suspected; Lowering Target to $126." In its analysis Credit Suisse stated that "we believe there is some merit to the whistleblower's report considering the source (Krebs on Security, a trusted cybersecurity

investigator) and given the UI customer impact from breaches of this sort, we believe there is reputational risk to UI which may begin impacting UI's sales generation starting in CY2Q21 (reflected in our latest model)." In explaining its Underperform (equivalent to a "sell" rating), the Credit Suisse noted that "Our Underperform thesis now hinges on very difficult revenue growth comps through FY2H21/FY22 and believe that the recent customer security breaches may weigh on revenue growth. Furthermore, there remains an outstanding SEC inquiry on UI, further pressing the company's management team for corporate governance updates."

40. Krebs on Security posted a follow up on April 4, 2021:[12] "Ubiquiti's statement largely confirmed the reporting here by not disputing any of the facts raised in the piece. And while it may seem that Ubiquiti is quibbling over whether data was in fact stolen, Adam said Ubiquiti can say there is no evidence that customer information was accessed because Ubiquiti failed to keep logs of who was accessing its databases."

D. Ubiquiti's Reputation Among Its Users Suffers In Response To Defendants' Concealment Of The Breach's Severity

41. After Krebs revealed that Ubiquiti had misled the public as to the severity of the breach, Ubiquiti's reputation suffered damage. For example, Mitchell Clark wrote in his March 31, 2021 *The Verge* article that:

> [T]he fact that the statement confirms some of what the whistleblower said while leaving the most worrying parts (e.g., the alleged cover-up, lack of logs, poor security practices, etc.) unaddressed makes me uncomfortable to be a Ubiquiti owner.
>
> The company's networking gear is (or was) trusted by many techies, myself included, because it promised full control over your home or small business network, without the fears of cloud-based solutions.

[12] https://krebsonsecurity.com/2021/04/ubiquiti-all-but-confirms-breach-response-iniquity/ (last accessed on November 11, 2021).

> Throughout this process, Ubiquiti has failed to communicate properly with its customers. The fact that it's not denying the allegations, and indicates that they could be true, suggests that the original email was, at the very least, an insufficient warning.

42. Although Ubiquiti restricted users' ability to comment on the Company's official response to Kreb's report, users in different topic threads commented that "Ubiquiti's failure in disclosing the deep extent of their data breach until it was forced upon them to fess up about it gives me grave concern about the integrity of this company's honesty and willingness to keep it's customer's best interests at the fore."[13] Another user commented in a different topic thread that "With UniFi's handling of breach and their treatment of customers with hardware, EOL, software, etc, thats what makes me wonder if we should move away from UniFi like many people here it seems." (sic).[14] Similarly, at least one Reddit.com thread was entitled "want to abandon ubiquiti after latest hack…"[15] In response, another user commented that "the level of mistrust many now have due to how they hid as much as possible from us leads to folks not wanting any of their products. Basically, if they would mislead us about a hack after it was finally reported on, how much can I trust that their devices haven't been left vulnerable to attacks or already been hacked?"

V. DEFENDANTS' MATERIALLY FALSE AND/OR MISLEADING STATEMENTS ISSUED DURING THE CLASS PERIOD

43. The Class Period begins on January 11, 2021. On that day, the Company issued a public notice stating that it had become aware of "unauthorized access to certain of our information technology systems hosted by a third party cloud provider." The notice, sent in an email to

---

[13] https://community.ui.com/questions/UniFi-Switch-Lite-16-PoE-Remains-Out-of-Stock-for-Over-a-Month/59f44c64-f92d-410e-a427-fea75ef2bb87 (last accessed November 10, 2021).

[14] https://community.ui.com/questions/3rd-party-NVR-software-for-unifi-cameras/5509e57e-31c7-48bd-8f3c-7782bd1e1fdb (last accessed November 10, 2021).

[15] https://www.reddit.com/r/HomeNetworking/comments/ml55vs/want_to_abandon_ubiquti_after_latest_hack/ (last accessed November 10, 2021).

customers and later republished on Ubiquiti's website[16] and by major tech media outlets, including Tech Crunch, The Verge, and ZDNet, stated:

> Dear Customer,
>
> We recently became aware of unauthorized access to certain of our information technology systems hosted by a third party cloud provider. ***We have no indication that there has been unauthorized activity with respect to any user's account.***
>
> ***We are not currently aware of evidence of access to any databases that host user data, but we cannot be certain that user data has not been exposed.*** This data may include your name, email address, and the one-way encrypted password to your account (in technical terms, the passwords are hashed and salted). The data may include your address and phone number if you have provided that to us.
>
> As a precaution we encourage you to change your password. We recommend that you also change your password on any website where you use the same user ID or password. Finally, we recommend that you enable two-factor authentication on your Ubiquiti accounts if you have not already done so.
>
> We apologize for, and deeply regret, any inconvenience this may cause you. We take the security of your information very seriously and appreciate your continued trust.
>
> Thank you,
>
> Ubiquiti Team

44. The above statements in the customer notice were false and misleading because the Company materially downplayed the seriousness of the true risks to the Company's network infrastructure, customer data, privacy and safety, and reputational and financial harm Ubiquiti suffered. The statements (a) "We have no indication that there has been unauthorized activity with respect to any user's account;" and (b) "We are not currently aware of evidence of access to any databases that host user data, but we cannot be certain that user data has not been exposed" are misleading because (1) Ubiquiti knew it could not possibly be aware of any evidence of access

[16] https://community.ui.com/questions/Account-Notification/96467115-49b5-4dd6-9517-f8cdbf6906f3 (last accessed November 11, 2021).

because they knowingly did not maintain access logs on its servers, contrary to standard operating procedures for similar tech companies; (2) Ubiquiti knew that it had no reasonable basis to make the statements, while at the same time, customers and investors believed that Ubiquiti was making that statement based on evidence, such as server logs, it had reviewed as part of its forensic investigation of the intrusion; (3) hackers had obtained administrative access to Ubiquiti's servers and obtained access to, among other things, all databases, all user database credentials, and secrets required to forge single sign-on (SSO) cookies; (4) as a result, intruders already had credentials needed to remotely access Ubiquiti's customers' systems.

VI. LOSS CAUSATION

45. Defendants' wrongful conduct, as alleged herein, directly and proximately caused the economic loss suffered by Plaintiff and the Class.

46. During the Class Period, Plaintiff and the Class purchased Ubiquiti's securities at artificially inflated prices and were damaged thereby. The price of the Company's securities significantly declined when the misrepresentations made to the market were revealed, causing investors' losses.

47. On March 30, 2021, at 2 pm eastern time, *Krebs on Security* published an article entitled "Whistleblower: Ubiquiti Breach 'Catastrophic'" stating that the Company had downplayed the data breach and that the "third-party cloud provider claim was a fabrication." The article cited a security professional at Ubiquiti (nicknamed "Adam") who had responded to the two-month breach beginning in December 2020, after he had raised concerns with the Company's whistleblower hotline and with European data protection authorities. According to Adam, the Company had been aware since December 2020 that attackers had "administrative access to all Ubiquiti AWS accounts, including . . . all user database credentials, and secrets required to forge single sign-on (SSO) cookies." The article stated:

According to Adam, the hackers obtained full read/write access to Ubiquiti databases at Amazon Web Services (AWS), which was the alleged "third party" involved in the breach. Ubiquiti's breach disclosure, he wrote, was "downplayed and purposefully written to imply that a 3rd party cloud vendor was at risk and that Ubiquiti was merely a casualty of that, instead of the target of the attack."

In its Jan. 11 public notice, Ubiquiti said it became aware of "unauthorized access to certain of our information technology systems hosted by a third party cloud provider," although it declined to name the third party.

[image omitted]

In reality, Adam said, the attackers had gained administrative access to Ubiquiti's servers at Amazon's cloud service, which secures the underlying server hardware and software but requires the cloud tenant (client) to secure access to any data stored there.

"They were able to get cryptographic secrets for single sign-on cookies and remote access, full source code control contents, and signing keys exfiltration," Adam said.

Adam says ***the attacker(s) had access to privileged credentials that were previously stored in the LastPass account of a Ubiquiti IT employee, and gained root administrator access to all Ubiquiti AWS accounts, including all S3 data buckets, all application logs, all databases, all user database credentials, and secrets required to forge single sign-on (SSO) cookies.***

Such access could have allowed the intruders to remotely authenticate to countless Ubiquiti cloud-based devices around the world. According to its website, Ubiquiti has shipped more than 85 million devices that play a key role in networking infrastructure in over 200 countries and territories worldwide.

Adam says ***Ubiquiti's security team picked up signals in late December 2020 that someone with administrative access had set up several Linux virtual machines that weren't accounted for.***

Then they found a backdoor that an intruder had left behind in the system.

When security engineers removed the backdoor account in the first week of January, the intruders responded by sending a message saying they wanted 50 bitcoin (~$2.8 million USD) in exchange for a promise to remain quiet about the breach. The attackers also provided proof they'd stolen Ubiquiti's source code, and pledged to disclose the location of another backdoor if their ransom demand was met.

Ubiquiti did not engage with the hackers, Adam said, and ultimately the incident response team found the second backdoor the extortionists had left in the system. The company would spend the next few days furiously rotating credentials for all

> employees, before Ubiquiti started alerting customers about the need to reset their passwords.
>
> But he maintains that instead of asking customers to change their passwords when they next log on — as the company did on Jan. 11 — Ubiquiti should have immediately invalidated all of its customer's credentials and forced a reset on all accounts, mainly because the intruders already had credentials needed to remotely access customer IoT systems.
>
> "Ubiquiti had negligent logging (no access logging on databases) so it was unable to prove or disprove what they accessed, but the attacker targeted the credentials to the databases, and created Linux instances with networking connectivity to said databases," Adam wrote in his letter. "Legal overrode the repeated requests to force rotation of all customer credentials, and to revert any device access permission changes within the relevant period."

48. The Krebs report was released at approximately 2 pm EST on March 30. With only two hours of trading left on the NYSE that day, the Company's stock price fell $27.78 per share, or 7.4%. As word of the Krebs Report spread, Ubiquiti's share price continued to fall another $50.70 per share, or 14.5%, on March 31, 2021, to close at $298.30 on March 31, 2021, all on unusually heavy trading volume.

49. On March 31, 2021, after the close of trading, Ubiquiti posted the following response to its website:

> As we informed you on January 11, we were the victim of a cybersecurity incident that involved unauthorized access to our IT systems. Given the reporting by Brian Krebs, there is newfound interest and attention in this matter, and we would like to provide our community with more information.
>
> At the outset, please note that nothing has changed with respect to our analysis of customer data and the security of our products since our notification on January 11. In response to this incident, we leveraged external incident response experts to conduct a thorough investigation to ensure the attacker was locked out of our systems.
>
> These experts identified no evidence that customer information was accessed, or even targeted. The attacker, who unsuccessfully attempted to extort the company by threatening to release stolen source code and specific IT credentials, never claimed to have accessed any customer information. This, along with other evidence, is why we believe that customer data was not the target of, or otherwise accessed in connection with, the incident.

> At this point, we have well-developed evidence that the perpetrator is an individual with intricate knowledge of our cloud infrastructure. As we are cooperating with law enforcement in an ongoing investigation, we cannot comment further.
>
> All this said, as a precaution, we still encourage you to change your password if you have not already done so, including on any website where you use the same user ID or password. We also encourage you to enable two-factor authentication on your Ubiquiti accounts if you have not already done so.
>
> Thanks,
>
> Team UI

50. That same day, the tech news website *The Verge* published an article criticizing Ubiquiti's response to the breach and To *Krebs on Security's* reporting:

> Ubiquiti, a company whose prosumer-grade routers have become synonymous with security and manageability, is being accused of covering up a "catastrophic" security breach — and after 24 hours of silence, the company has now issued a statement that doesn't deny any of the whistleblower's claims.
>
> Originally, Ubiquiti emailed its customers about a supposedly minor security breach at a "third party cloud provider" on January 11th, but noted cybersecurity news site KrebsOnSecurity is reporting that the breach was actually far worse than Ubiquiti let on. A whistleblower from the company who spoke to Krebs claimed that Ubiquiti itself was breached, and that the company's legal team prevented efforts to accurately report the dangers to customers.
>
> It's worth reading Krebs' report to see the full allegations, but the summary is that hackers got full access to the company's AWS servers — since Ubiquiti allegedly left root administrator logins in an LastPass account — and they could have been able to access any Ubiquiti networking gear that customers had set up to control via the company's cloud service (now seemingly required on some of the company's new hardware).
>
> "They were able to get cryptographic secrets for single sign-on cookies and remote access, full source code control contents, and signing keys exfiltration," the source told Krebs.
>
> When Ubiquiti finally issued a statement this evening, it wasn't a reassuring one — it's wildly insufficient. The company reiterated its point that it had no evidence to indicate that any user data had been accessed or stolen. But as Krebs points out, the whistleblower explicitly stated that the company doesn't keep logs, which would act as that evidence, on who did or didn't access the hacked servers. Ubiquiti's statement also confirms that the hacker did try to extort it for money, but doesn't address the allegations of a cover up.

…

> The other thing you'll notice is that Ubiquiti is no longer pinning this on a "third party cloud provider." The company admits that its own IT systems were accessed. But it doesn't address much else, and the fact that the statement confirms some of what the whistleblower said while leaving the most worrying parts (e.g., the alleged cover-up, lack of logs, poor security practices, etc.) unaddressed makes me uncomfortable to be a Ubiquiti owner.
>
> The company's networking gear is (or was) trusted by many techies, myself included, because it promised full control over your home or small business network, without the fears of cloud-based solutions.
>
> Throughout this process, Ubiquiti has failed to communicate properly with its customers. The fact that it's not denying the allegations, and indicates that they could be true, suggests that the original email was, at the very least, an insufficient warning. It encouraged users to change their passwords — according to Krebs, a more appropriate response would be immediately locking all accounts and requiring a password reset. Even today, the company is simply encouraging users to change their passwords and enable two-factor authentication.

51. Thus, Ubiquiti did not challenge and essentially admitted to the substance of Krebs On Security's reporting. On this news Ubiquiti's stock fell another $9.15 per share, or 3%, to close at $289.15 per share on April 1, 2021, on unusually heavy trading volume.

52. On April 4, 2021, *Krebs on Security* published a follow-up article to note that Ubiquiti's response "confirms and reinforces th[e] claims" from the March 30, 2021 article. Specifically, it stated:

> Ubiquiti finally responded on Mar. 31, in a post signed "Team UI" on the company's community forum online.
>
> "Nothing has changed with respect to our analysis of customer data and the security of our products since our notification on January 11. In response to this incident, we leveraged external incident response experts to conduct a thorough investigation to ensure the attacker was locked out of our systems."
>
> "These experts identified no evidence that customer information was accessed, or even targeted. The attacker, who unsuccessfully attempted to extort the company by threatening to release stolen source code and specific IT credentials, never claimed to have accessed any customer information. This, along with other evidence, is why we believe that customer data was not the target of, or otherwise accessed in connection with, the incident."

* * *

> Ubiquiti's statement largely confirmed the reporting here by not disputing any of the facts raised in the piece. And while it may seem that Ubiquiti is quibbling over whether data was in fact stolen, Adam said Ubiquiti can say there is no evidence that customer information was accessed because Ubiquiti failed to keep logs of who was accessing its databases.

VII. ADDITIONAL SCIENTER ALLEGATIONS PERTAINING TO DEFENDANT PERA

53. Defendant Pera had motive to commit fraud because he posted 25% of his shares of Ubiquiti common stock as collateral for loans. Pursuant to the agreements underlying those loans, if Ubiquiti stock drops below a certain level, Pera will be forced to sell his shares of Ubiquiti stock to repay the loans. As the 10-Q that Ubiquiti filed on February 5, 2021, stated:

> As of February 5, 2021, Mr. Pera beneficially owned 56,278,181 shares of our common stock. These shares are eligible for resale into the public market within the restrictions imposed by Rule 144 under the Securities Act of 1933. Sales of a significant amount of Mr. Pera's shares could adversely affect the market price for our common stock. Mr. Pera had informed us he has entered into arrangements under which he has pledged up to 25% of the shares of our common stock that he beneficially owns to secure loans with financial institutions. Mr. Pera had also indicated these loans have or will have various requirements to repay all or a portion of the loan upon the occurrence of various events, including when the price of the common stock goes below certain specified levels. Mr. Pera may need to sell shares of our common stock to meet these repayment requirements. Upon a default under one or more of these loans, the lender could sell the pledged shares into the market without limitation on volume or manner of sale. Sales of shares by Mr. Pera to reduce his loan balance or the lenders upon foreclosure are likely to adversely affect our stock price. Mr. Pera has also indicated to us that he may in the future from time to time pledge additional shares of common stock as collateral for margin or other loans, enter into derivative transactions based on the value of our common stock, dispose of shares of common stock, otherwise monetize shares of his common stock and/or engage in other transactions relating to shares of our common stock and/or other securities of the company. Any of these activities by Mr. Pera may adversely affect the price of our common stock. However, Mr. Pera has also indicated that he intends to continue to own at least a majority of our outstanding shares of common stock.

54. Although the details of Pera's loans and their repayment requirements, including the specified Ubiquiti stock price level at which these repayment requirements would be triggered,

are not publicly available, Ubiquiti first disclosed that "Pera has informed us he intends to pledge up to 28% of the shares of our common stock that he beneficially owns to secure one or more loans with one or more financial institutions" in Ubiquiti's Form 10-Q filed on May 10, 2018.

55. The value of the 25% of his shares that he pledged to collateralize the loans was approximately $1,145,824 as of May 10, 2018 based on a closing price of $81.44 per share.

56. These loans created a motive to inflate the price of Ubiquiti stock so as not to trigger the thresholds where Pera would be required to sell his shares.

57. Defendant Pera's scienter is also established by his unusually tight control of Ubiquiti as its CEO, Chairman, and founder. In addition, because Pera chose to run theCompany without the layers of oversight that ordinary public companies have, he is even more involved in all aspects of its operations than an ordinary CEO would be. Ubiquiti states that as the Company's founder, Chairman, CEO, and majority owner, Pera "is able to exercise voting rights with respect to a majority of the voting power of our outstanding stock and therefore has the ability to control the outcome of matters submitted to our stockholders for approval, including the election of directors and any merger, consolidation, or sale of all or substantially all of our assets. In addition, Mr. Pera has the ability to control the management and major strategic investments of our company as a result of his position as our Chief Executive Officer and his ability to control the election or replacement of our directors. . . . As a board member and officer, Mr. Pera owes a fiduciary duty to our stockholders and must act in good faith in a manner he reasonably believes to be in the best interests of our stockholders. As a stockholder, even a controlling stockholder, Mr. Pera is entitled to vote his shares in his own interests, which may not always be in the interests of our stockholders generally."

58. Similarly, Pera stated at the Company's September 26, 2017 Investor Day that "I don't want to be the leader in the movies that sits up high in a castle and watches all of his soldiers, who he feels expendable get killed off one by one. I want to be the guy leading by example. I want to be the guy on the battlefield. And I think that top-down accountability is very important because when you have the small teams and something goes wrong, the worst thing forculture is somebody saying, 'Well, that's not my job'. If somebody sees a problem, they have to attack it. Just like I attack it. I don't consider myself lower -- above any job. I'll go into the forums, I'll go into the lab, I'll rework products, I don't care. I want that culture. And that's why Ido the things I do."

VIII. CORPORATE SCIENTER ALLEGATIONS

58. The Company is liable for the acts of the Individual Defendants and its other employees and agents under the doctrine of *respondeat superior* and common law principles of agency because all of the wrongful acts complained of herein were carried out within the scope of their employment and/or agency.

59. The scienter of the Individual Defendants and other employees and agents of the Company is similarly imputed to the Company under the corporate scienter doctrine, *respondeat superior*, and agency principles.

60. Aside from the scienter of the Individual Defendants, the facts alleged herein raise a strong inference of corporate scienter as to Ubiquiti as an entity. Corporate scienter may be alleged independent of individual defendants where a statement is made or approved by a corporate official sufficiently knowledgeable about the company to know the statement was false or misleading. Here, the statements alleged were made to the investing public regarding the Company's operations, internal controls, finances and business practices—all important topics that would necessarily require approval by appropriate corporate officers.

IX. CLASS ACTION ALLEGATIONS

61. Plaintiff brings this action as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3) on behalf of a class, consisting of all persons and entities that purchased or otherwise acquired Ubiquiti securities between January 11, 2021 and March 30, 2021, inclusive, and who were damaged thereby (the "Class"). Excluded from the Class are Defendants, the officers and directors of the Company, at all relevant times, members of their immediate families and their legal representatives, heirs, successors, or assigns, and any entity in which Defendants have or had a controlling interest.

62. The members of the Class are so numerous that joinder of all members is impracticable. Throughout the Class Period, Ubiquiti's shares actively traded on the NYSE. While the exact number of Class members is unknown to Plaintiff at this time and can only be ascertained through appropriate discovery, Plaintiff believes that there are at least hundreds or thousands of members in the proposed Class. Millions of Ubiquiti shares were traded publicly during the Class Period on the NYSE. As of February 3, 2021, Ubiquiti has 62,809,182 shares of common stock outstanding. Record owners and other members of the Class may be identified from records maintained by Ubiquiti or its transfer agent and may be notified of the pendency of this action by mail, using the form of notice similar to that customarily used in securities class actions.

63. Plaintiff's claims are typical of the claims of the members of the Class as all members of the Class are similarly affected by Defendants' wrongful conduct in violation of federal law that is complained of herein.

64. Plaintiff will fairly and adequately protect the interests of the members of the Class and has retained counsel competent and experienced in class and securities litigation.

65. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual members of the Class. Among the questions of law and fact common to the Class are:

a. whether the federal securities laws were violated by Defendants' acts as alleged herein;

b. whether statements made by Defendants to the investing public during the Class Period omitted and/or misrepresented material facts about the business, operations, and prospects of Ubiquiti;

c. whether Defendants knew or deliberately disregarded that their statements were false and misleading;

d. whether the price of Ubiquiti securities were artificially inflated because of Defendants' conduct complained of herein; and

e. to what extent the members of the Class have sustained damages and the proper measure of damages.

66. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation makes it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in the management of this action as a class action.

X. APPLICABILITY OF PRESUMPTION OF RELIANCE (FRAUD-ON-THE-MARKET DOCTRINE)

67. Plaintiff brings this action as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3) on behalf of a class consisting of all persons other than defendants who acquired Ubiquiti securities publicly traded on the New York Stock Exchange market during the

Class Period, and who were damaged thereby (the "Class"). Excluded from the Class are Defendants, the officers and directors of Ubiquiti and its subsidiaries, members of the Individual Defendants' immediate families and their legal representatives, heirs, successors or assigns and any entity in which Defendants have or had a controlling interest.

68. The members of the Class are so numerous that joinder of all members is impracticable. Throughout the Class Period, Ubiquiti securities were actively traded on the NYSE. While the exact number of Class members is unknown to Plaintiff at this time and can be ascertained only through appropriate discovery, Plaintiff believes that there are hundreds, if not thousands of members in the proposed Class.

69. Plaintiff's claims are typical of the claims of the members of the Class as all members of the Class are similarly affected by defendants' wrongful conduct in violation of federal law that is complained of herein.

70. Plaintiff will fairly and adequately protect the interests of the members of the Class and has retained counsel competent and experienced in class and securities litigation. Plaintiff has no interests antagonistic to or in conflict with those of the Class.

71. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual members of the Class. Among the questions of law and fact common to the Class are:

- whether the federal securities laws were violated by Defendants' acts as alleged herein;
- whether statements made by Defendants to the investing public during the Class Period misrepresented material facts about the financial condition, business, operations, and management of the Company;

- whether Defendants' public statements to the investing public during the Class Period omitted material facts necessary to make the statements made, in light of the circumstances under which they were made, not misleading;
- whether the Individual Defendants caused the Company to issue false and misleading public statements during the Class Period;
- whether Defendants acted knowingly or recklessly in issuing false and misleading public statements during the Class Period;
- whether the prices of the Company's securities during the Class Period were artificially inflated because of the Defendants' conduct complained of herein; and
- whether the members of the Class have sustained damages and, if so, what is the proper measure of damages.

72. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in the management of this action as a class action.

73. Plaintiff will rely, in part, upon the presumption of reliance established by the fraud-on-the-market doctrine in that:

- Defendants made public misrepresentations or failed to disclose material facts during the Class Period;
- the omissions and misrepresentations were material;
- the Company's securities are traded in efficient markets;

- the Company's securities were liquid and traded with moderate to heavy volume during the Class Period;
- the Company's securities traded on the NYSE market, and was covered by at least five analysts;
- the company's common stock traded with heavy volume, with 1.9% of the company's float trading daily on average;
- the misrepresentations and omissions alleged would tend to induce a reasonable investor to misjudge the value of the Company's securities; and
- Plaintiff and members of the Class purchased and/or sold the Company's securities between the time the Defendants failed to disclose or misrepresented material facts and the time the true facts were disclosed, without knowledge of the omitted or misrepresented facts.

74. Based upon the foregoing, Plaintiff and the members of the Class are entitled to a presumption of reliance upon the integrity of the market.

75. Alternatively, Plaintiff and the members of the Class are entitled to the presumption of reliance established by the Supreme Court in *Affiliated Ute Citizens of the State of Utah v. United States*, 406 U.S. 128, 92 S. Ct. 2430 (1972), as Defendants omitted material information in their Class Period statements in violation of a duty to disclose such information, as detailed above.

XI. INAPPLICABILITY OF THE STATUTORY SAFE HARBOR AND BESPEAKS CAUTION DOCTRINE

76. The statutory safe harbor and/or bespeaks caution doctrine applicable to forward-looking statements under certain circumstances does not apply to any of the allegedly false statements pleaded in this Complaint.

77. The statements alleged to be false and misleading herein all relate to then-existing facts and conditions. In addition, to the extent certain of the statements alleged to be false may be characterized as forward looking, they were not identified as "forward-looking statements" when made and there were no meaningful cautionary statements identifying important factors that could cause actual results to differ materially from those in the purportedly forward-looking statements.

78. In the alternative, to the extent that the statutory safe harbor is determined to apply to any forward-looking statements pleaded herein, Defendants are liable for those false forward-looking statements because at the time each of those forward-looking statements was made, the speaker had actual knowledge that the forward-looking statement was materially false or misleading, and/or the forward-looking statement was authorized or approved by an executive officer of Ubiquiti who knew that the statement was false when made.

XII. CLAIMS FOR RELIEF

FIRST CLAIM
Violation Of Section 10(b)
Of The Exchange Act And Rule 10b-5 Promulgated Thereunder
Against Defendant Ubiquiti Inc. And The Individual Defendants

79. Plaintiff repeats and re-alleges each and every allegation contained above as if fully set forth herein.

80. During the Class Period, Defendants carried out a plan, scheme and course of conduct which was intended to and, throughout the Class Period, did: (i) deceive the investing public, including Plaintiff and other Class members, as alleged herein; and (ii) cause Plaintiff and other members of the Class to purchase Ubiquiti's securities at artificially inflated prices. In furtherance of this unlawful scheme, plan and course of conduct, Defendants, and each defendant, took the actions set forth herein.

81. Defendants (i) employed devices, schemes, and artifices to defraud; (ii) made untrue statements of material fact and/or omitted to state material facts necessary to make the statements not misleading; and (iii) engaged in acts, practices, and a course of business which operated as a fraud and deceit upon the purchasers of the Company's securities in an effort to maintain artificially high market prices for Ubiquiti's securities in violation of Section 10(b) of the Exchange Act and Rule 10b-5. All Defendants are sued either as primary participants in the wrongful and illegal conduct charged herein or as controlling persons as alleged below.

82. Defendants, individually and in concert, directly and indirectly, by the use, means or instrumentalities of interstate commerce and/or of the mails, engaged and participated in a continuous course of conduct to conceal adverse material information about Ubiquiti's financial well-being and prospects, as specified herein.

83. Defendants employed devices, schemes and artifices to defraud, while in possession of material adverse non-public information and engaged in acts, practices, and a course of conduct as alleged herein in an effort to assure investors of Ubiquiti's value and performance and continued substantial growth, which included the making of, or the participation in the making of, untrue statements of material facts and/or omitting to state material facts necessary in order to make the statements made about Ubiquiti and its business operations and future prospects in light of the circumstances under which they were made, not misleading, as set forth more particularly herein, and engaged in transactions, practices and a course of business which operated as a fraud and deceit upon the purchasers of the Company's securities during the Class Period.

84. Each of the Individual Defendants' primary liability and controlling person liability arises from the following facts: (i) the Individual Defendants were high-level executives and/or directors at the Company during the Class Period and members of the Company's management

team or had control thereof; (ii) each of these defendants, by virtue of their responsibilities and activities as a senior officer and/or director of the Company, was privy to and participated in the creation, development and reporting of the Company's internal budgets, plans, projections and/or reports; (iii) each of these defendants enjoyed significant personal contact and familiarity with the other defendants and was advised of, and had access to, other members of the Company's management team, internal reports and other data and information about the Company's finances, operations, and sales at all relevant times; and (iv) each of these defendants was aware of the Company's dissemination of information to the investing public which they knew and/or recklessly disregarded was materially false and misleading.

85. Defendants had actual knowledge of the misrepresentations and/or omissions of material facts set forth herein, or acted with reckless disregard for the truth in that they failed to ascertain and to disclose such facts, even though such facts were available to them. Such defendants' material misrepresentations and/or omissions were done knowingly or recklessly and for the purpose and effect of concealing Ubiquiti's financial well-being and prospects from the investing public and supporting the artificially inflated price of its securities. As demonstrated by Defendants' overstatements and/or misstatements of the Company's business, operations, financial well-being, and prospects throughout the Class Period, Defendants, if they did not have actual knowledge of the misrepresentations and/or omissions alleged, were reckless in failing to obtain such knowledge by deliberately refraining from taking those steps necessary to discover whether those statements were false or misleading.

86. As a result of the dissemination of the materially false and/or misleading information and/or failure to disclose material facts, as set forth above, the market price of Ubiquiti's securities was artificially inflated during the Class Period. In ignorance of the fact that

market prices of the Company's securities were artificially inflated, and relying directly or indirectly on the false and misleading statements made by Defendants, or upon the integrity of the market in which the securities trades, and/or in the absence of material adverse information that was known to or recklessly disregarded by Defendants, but not disclosed in public statements by Defendants during the Class Period, Plaintiff and the other members of the Class acquired Ubiquiti's securities during the Class Period at artificially high prices and were damaged thereby.

87. At the time of said misrepresentations and/or omissions, Plaintiff and other members of the Class were ignorant of their falsity, and believed them to be true. Had Plaintiff and the other members of the Class and the marketplace known the truth regarding the problems that Ubiquiti was experiencing, which were not disclosed by Defendants, Plaintiff and other members of the Class would not have purchased or otherwise acquired their Ubiquiti securities, or, if they had acquired such securities during the Class Period, they would not have done so at the artificially inflated prices which they paid.

88. By virtue of the foregoing, Defendants violated Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder.

89. As a direct and proximate result of Defendants' wrongful conduct, Plaintiff and the other members of the Class suffered damages in connection with their respective purchases and sales of the Company's securities during the Class Period.

SECOND CLAIM
Violation of Section 20(a) of The Exchange Act
Against the Individual Defendants

90. Plaintiff repeats and re-alleges each and every allegation contained above as if fully set forth herein.

91. Individual Defendants acted as controlling persons of Ubiquiti within the meaning of Section 20(a) of the Exchange Act as alleged herein. By virtue of their high-level positions and

their ownership and contractual rights, participation in, and/or awareness of the Company's operations and intimate knowledge of the false financial statements filed by the Company with the SEC and disseminated to the investing public, Individual Defendants had the power to influence and control and did influence and control, directly or indirectly, the decision-making of the Company, including the content and dissemination of the various statements which Plaintiff contends are false and misleading. Individual Defendants were provided with or had unlimited access to copies of the Company's reports, press releases, public filings, and other statements alleged by Plaintiff to be misleading prior to and/or shortly after these statements were issued and had the ability to prevent the issuance of the statements or cause the statements to be corrected.

92. In particular, Individual Defendants had direct and supervisory involvement in the day-to-day operations of the Company and, therefore, had the power to control or influence the particular transactions giving rise to the securities violations as alleged herein, and exercised the same.

93. As set forth above, Ubiquiti and Individual Defendants each violated Section 10(b) and Rule 10b-5 by their acts and omissions as alleged in this Complaint. By virtue of their position as controlling persons, Individual Defendants are liable pursuant to Section 20(a) of the Exchange Act. As a direct and proximate result of Defendants' wrongful conduct, Plaintiff and other members of the Class suffered damages in connection with their purchases of the Company's securities during the Class Period.

XIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief and judgment, as follows:

a. Determining that this action is a proper class action under Rule 23 of the Federal Rules of Civil Procedure;

b. Awarding compensatory damages in favor of Plaintiff and the other Class members against all defendants, jointly and severally, for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

c. Awarding Plaintiff and the Class their reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

d. Such other and further relief as the Court may deem just and proper.

XIV. JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury.

Dated: November 12, 2021

THE ROSEN LAW FIRM, P.A.

By: /s/ Jonathan Stern

Jonathan Stern, Esq. (JS 3683)
Phillip Kim, Esq. (PK 9384)
Laurence M. Rosen, Esq. (LR 5733)
275 Madison Avenue, 40th Floor
New York, New York 10016
Telephone: (212) 686-1060
Facsimile: (212) 202-3827
Email: jstern@rosenlegal.com
pkim@rosenlegal.com
lrosen@rosenlegal.com

Counsel for Lead Plaintiff Irit Lukomski